

# Hardening Systems in an Era of Pervasive Networking

**Hal Jespersen**  
**Chief Technologist,**  
**Sun ONE Products**



# Agenda





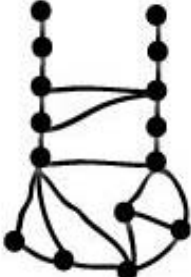

- Services Architectures and the Future of the Internet
- Sun ONE – Open Net Environment
  - Web Services and Services on Demand
  - Liberty Alliance Federated Identity Standards
- N1 Dynamic Service Provisioning
- Jini, JXTA, and the Future of Dynamic Configuration
- Some Tips on Hardening Systems

# Eight Fallacies of Distributed Computing\*

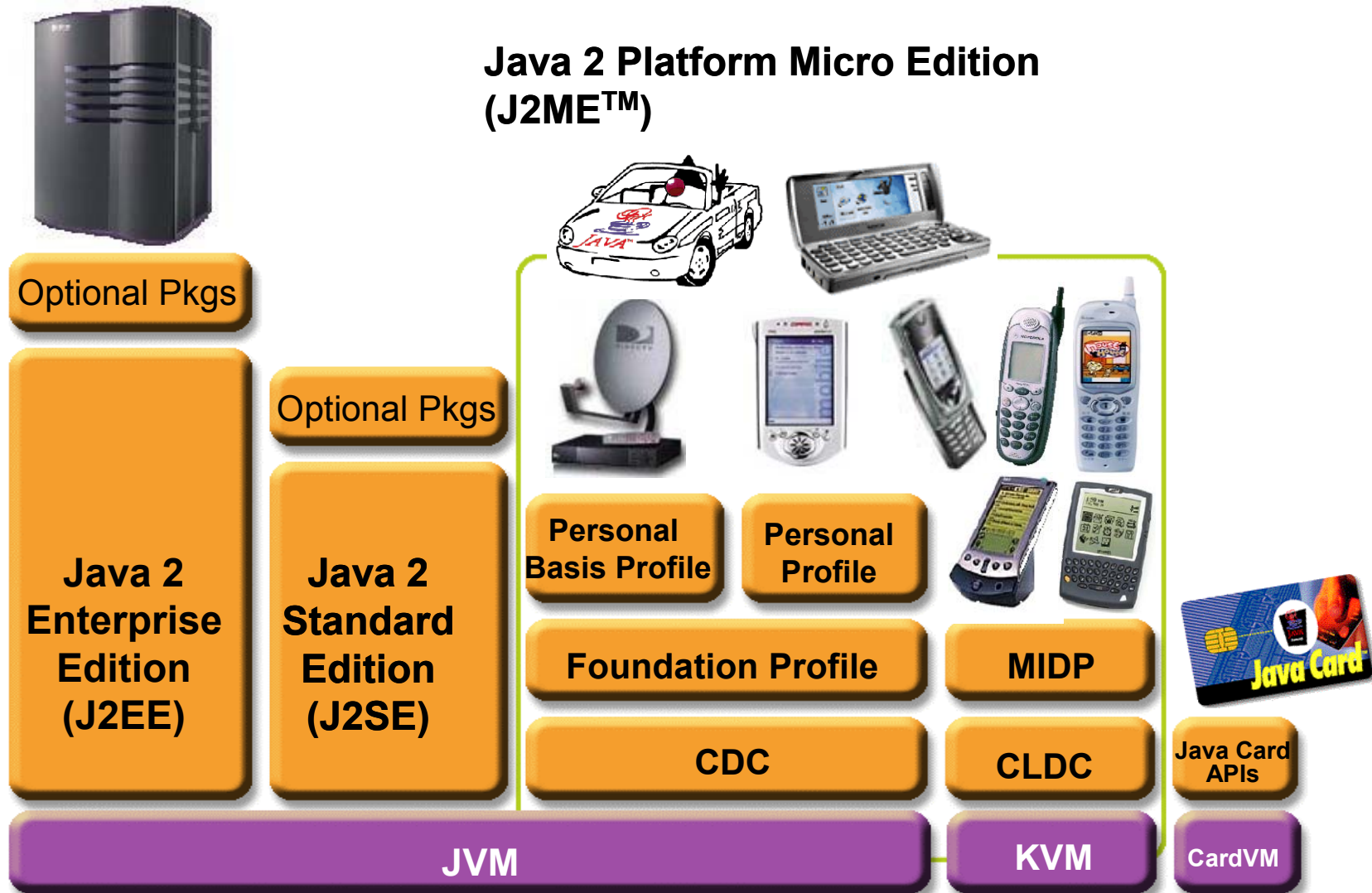
1. The network is reliable
2. Latency is zero
3. Bandwidth is infinite
4. The network is secure
5. Topology doesn't change
6. There is one administrator
7. Transport cost is zero
8. The network is homogeneous

\* Peter Deutsch

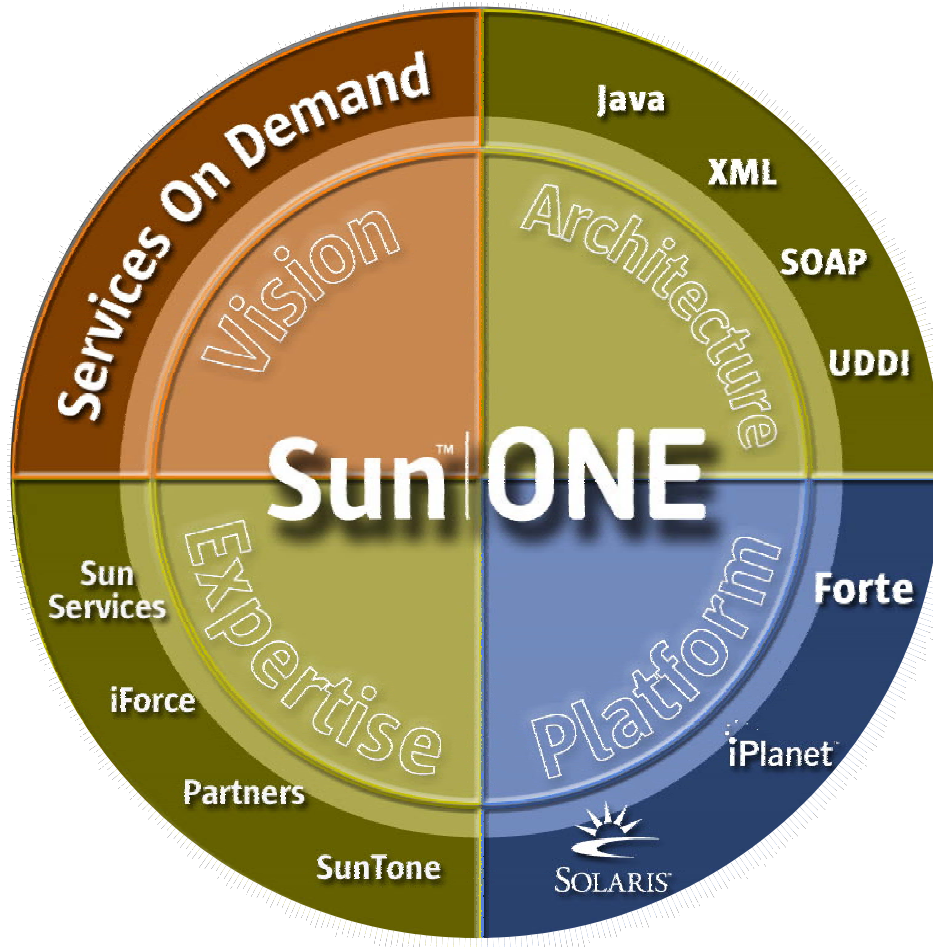
# Evolution of Networked Computing

Catch Phrase	The Network is the computer	Objects	Legacy to the Web	The Computer is the Network	Network of embedded things	Network of things
Scale	100s	1000s	1000000s	10000000s	100000000s	100000000s
When/ Peak	1984/ 1987	1990/ 1993	1996/ 1999	2001/2003	1998/2004	2004/2007
Leaf Protocol(s)	X	X	+HTTP (+JVM)	+XML, Portal	+RMI	Unknown
Directory(s)	NIS, NIS+	+CDS	+LDAP(*)	+UDDI	+Jini	+?
Session	RPC, XDR	+CORBA	+CORBA, RMI	+SOAP, XML	+RMI/ Jini	+?
Schematic						

# The Java™ 2 Platform

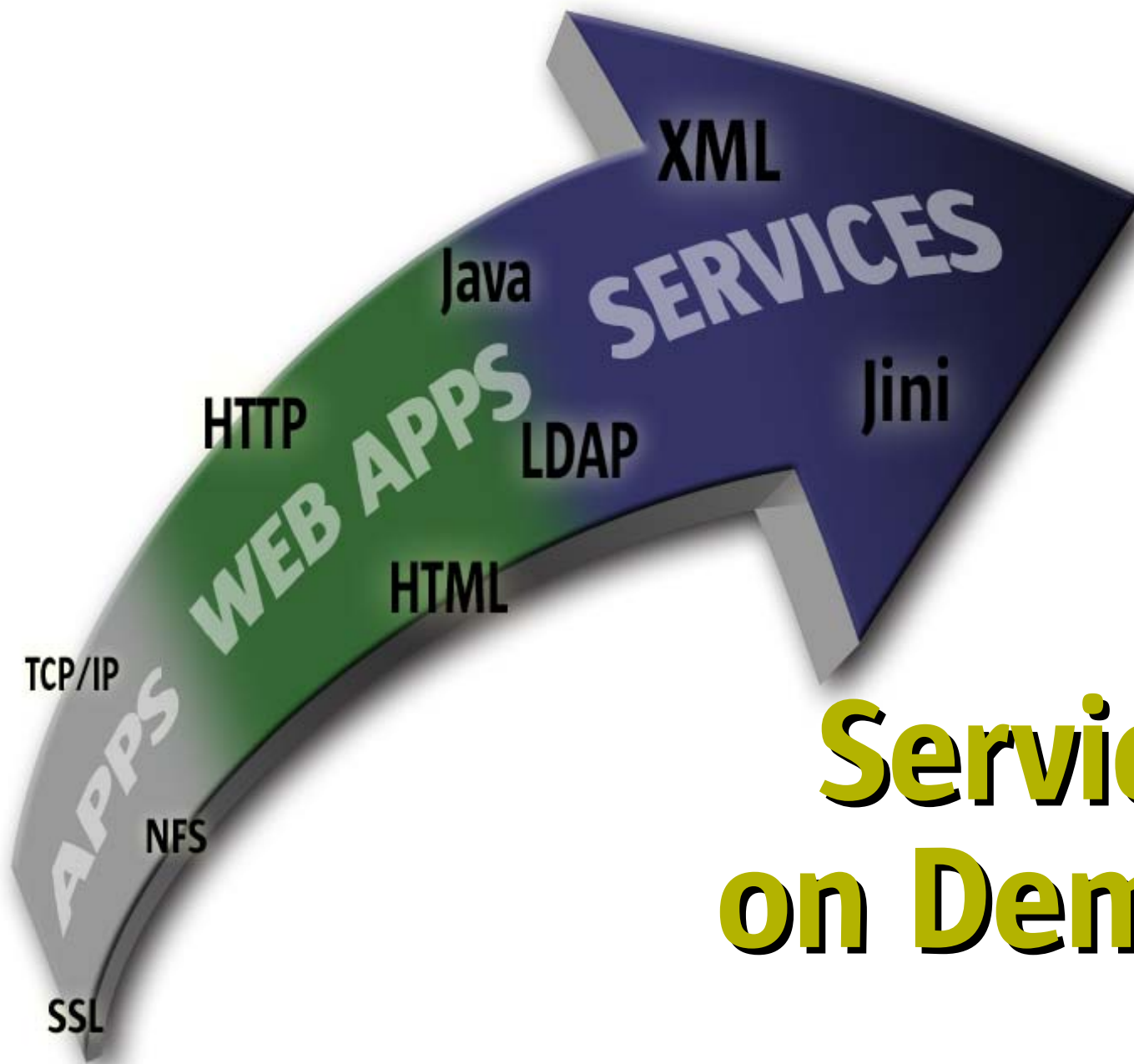


# Sun ONE – Open Net Environment



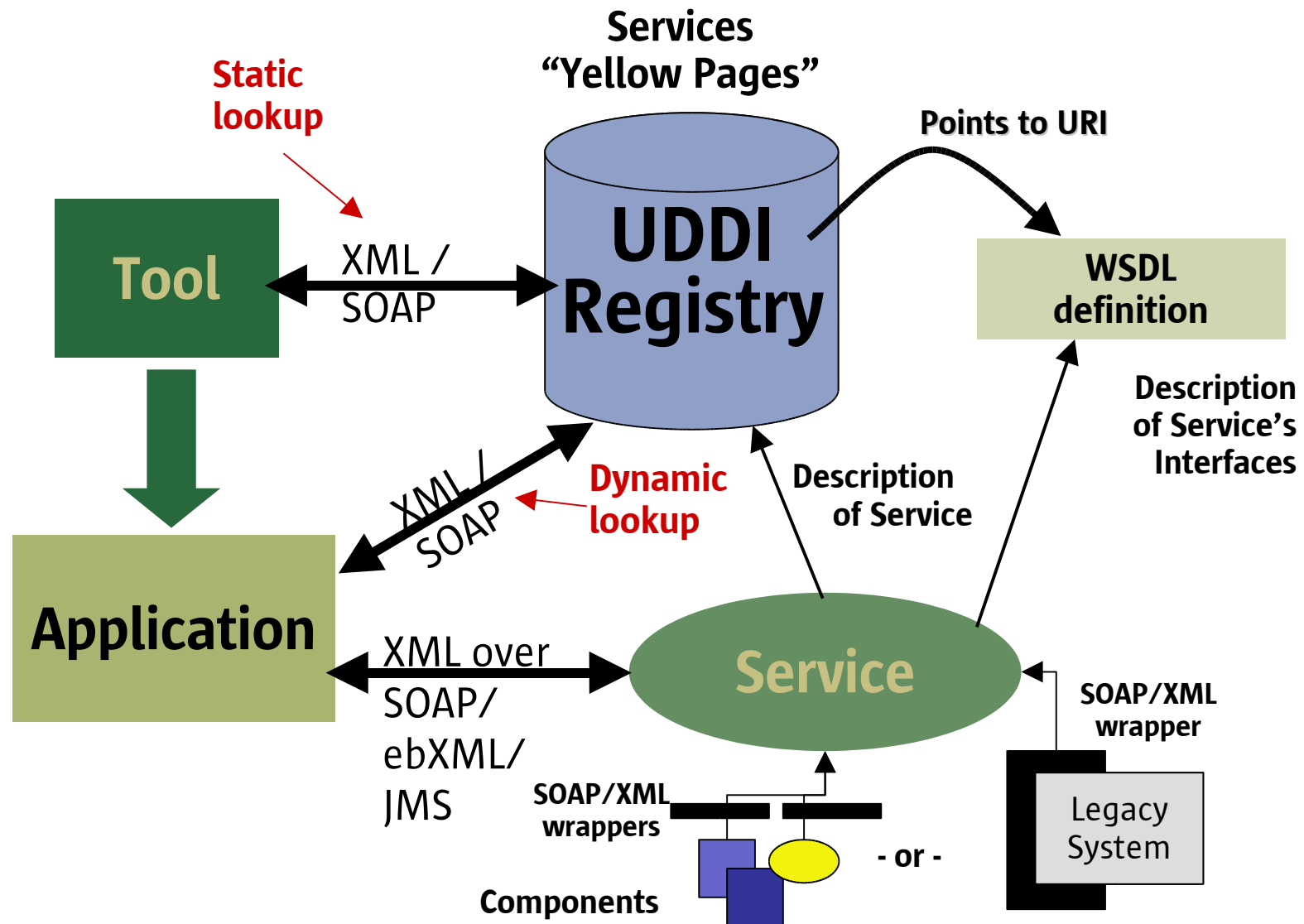
Download Sun ONE Architecture Guide from  
<http://www.sun.com/sunone/docs/arch/>





# Services on Demand

# Web Services

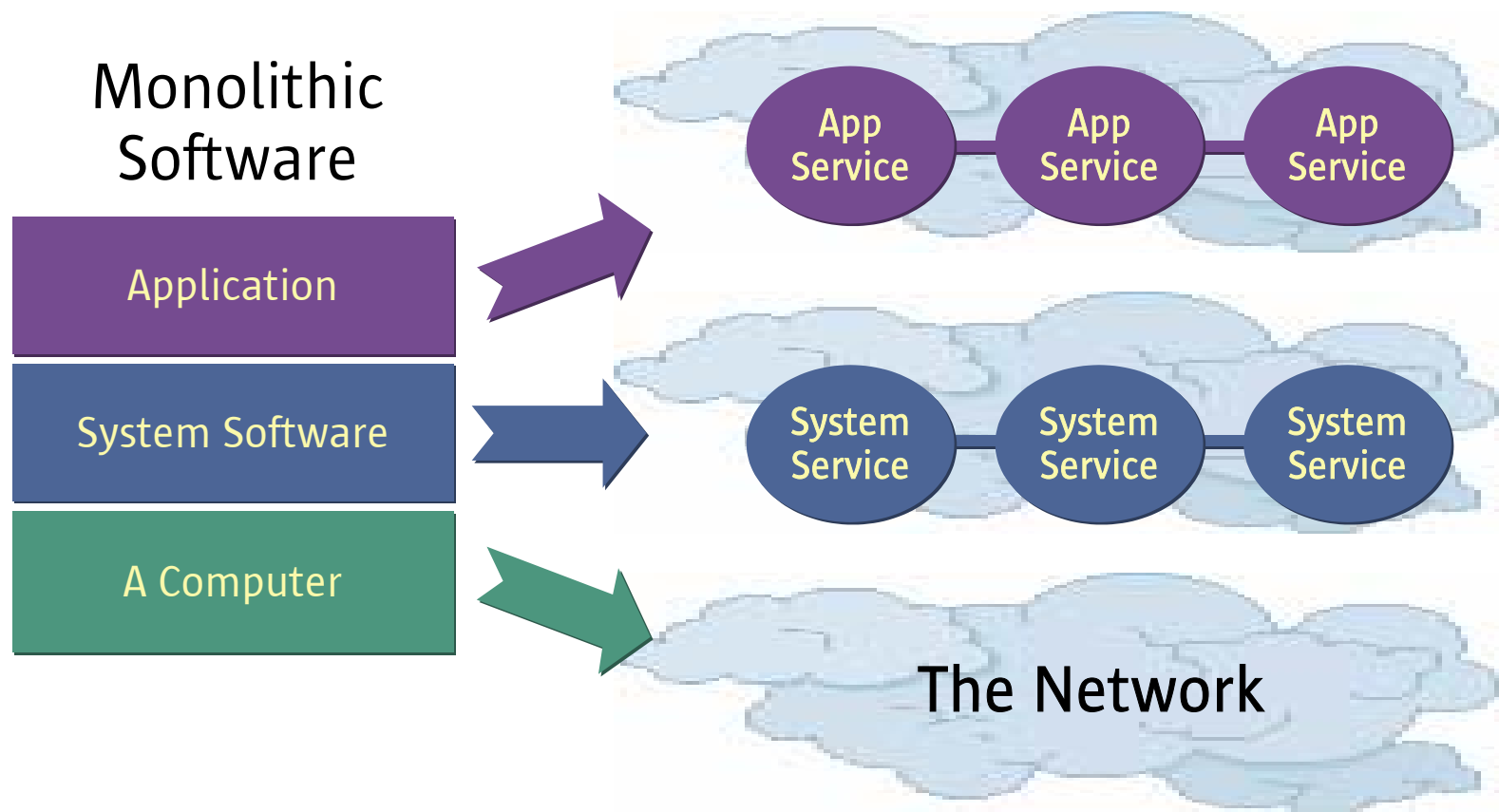




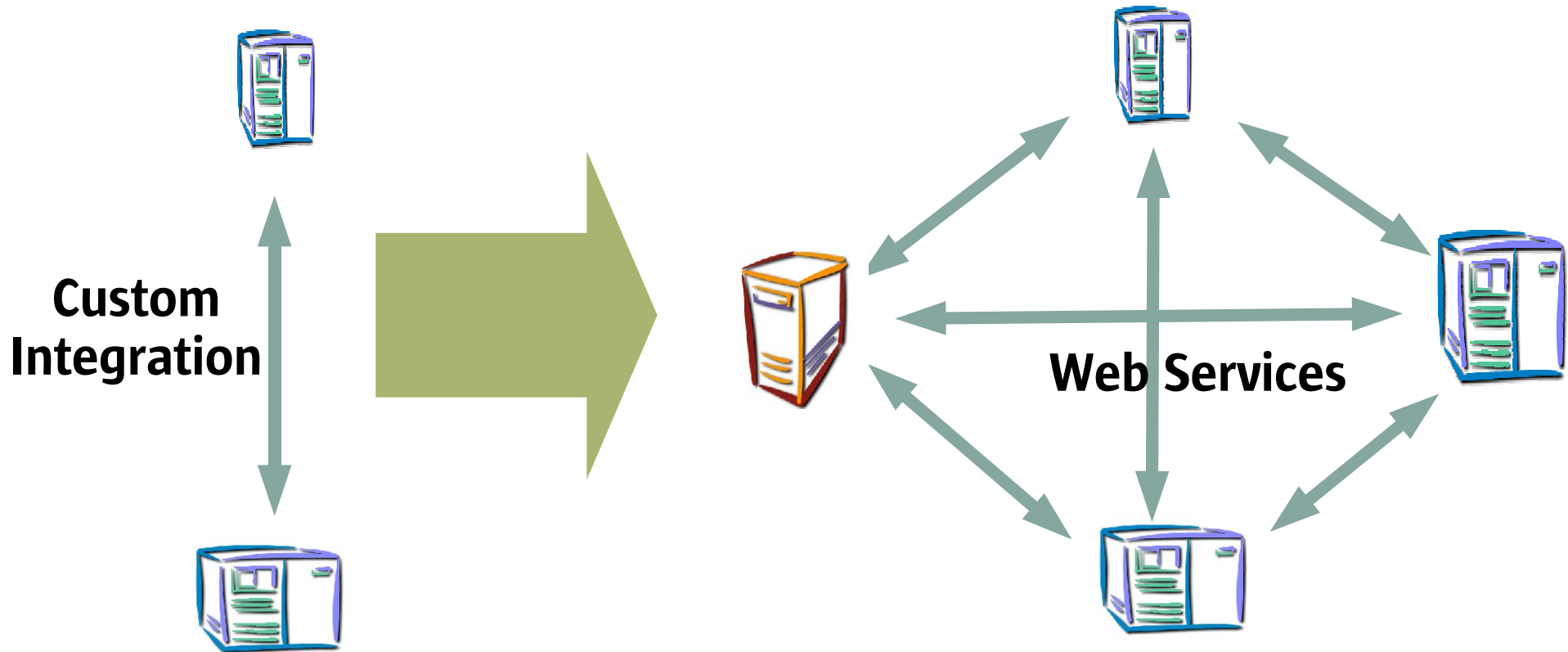
# Impact on Software

## “Application Dis-Integration”

### Web Services



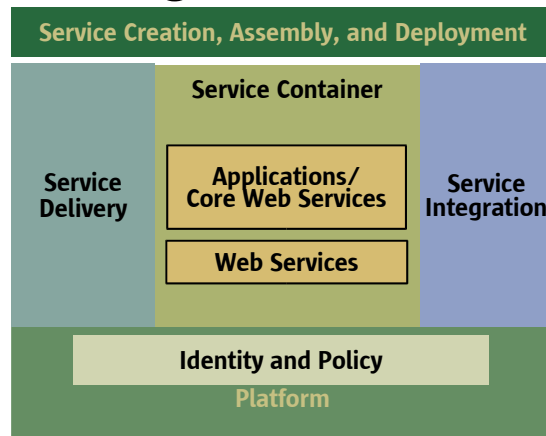
# Impact on Integration: Trigger the Network Effect



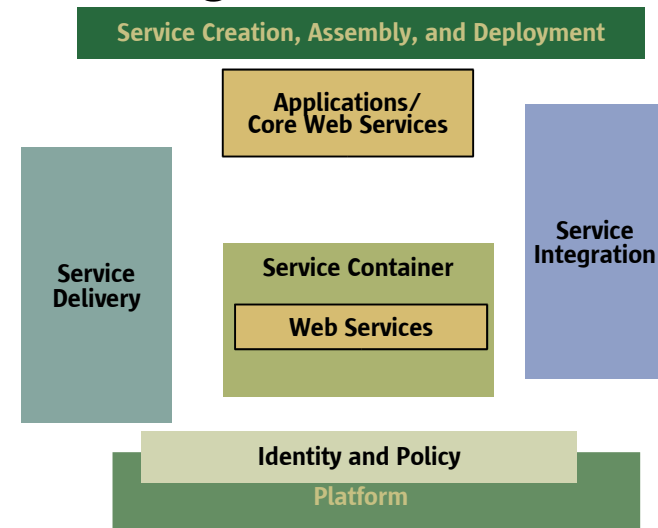
***Metcalfe's Law: The value of the network is proportional to the square of the number of users***

# Sun ONE Architecture: Integrated, Integratable

## *Integrated Stack*



## *Integratable Stack*

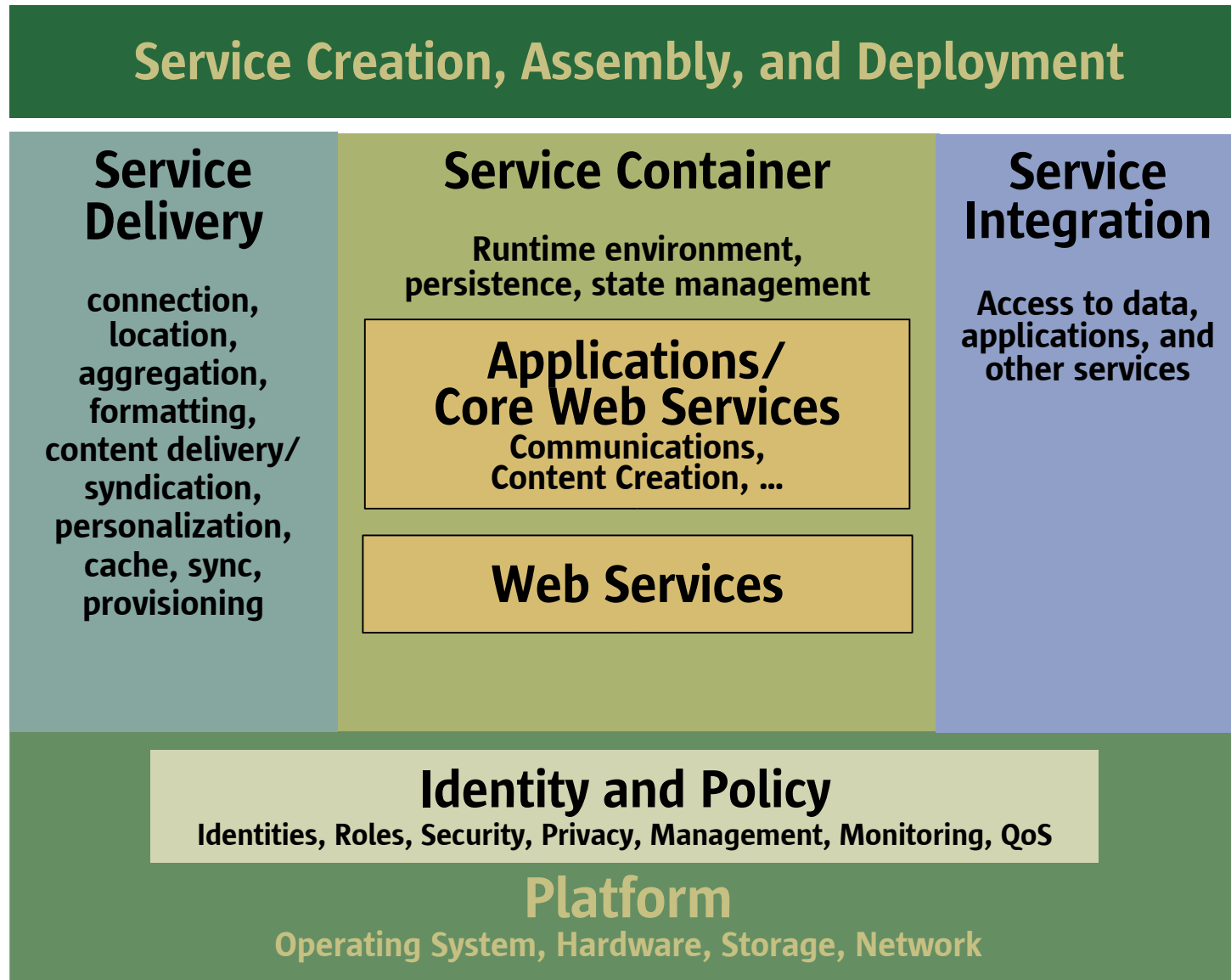


# Phases of Adoption

How will enterprises adopt web services technologies?

<b>Phase 1</b>	<b>Web applications and basic XML services infrastructure</b>
<b>Phase 2</b>	<b>Web services for enterprise internal integration, including B2E and enterprise-managed, bilateral B2B</b>
<b>Phase 3</b>	<b>Web services extended externally from the enterprise for dynamic B2C and B2B</b>

# Services Stack – Creating Services on Demand



# Integrated Stack

**Service Creation, Assembly, and Deployment**  
Sun ONE tools

## Service Delivery

Sun ONE Portal  
Server, Application  
Framework

## Service Container

Sun ONE Web, App Servers

**Applications/  
Core Web Services**  
Sun ONE  
Communications Apps

**Web Services**  
Sun ONE Web, App Servers

## Service Integration

Sun ONE App  
Server,  
Integration  
Servers,  
Directory/  
Registry Servers

## Identity and Policy

Sun ONE Directory Server, Identity Server, Sun Mgmt Frmwk

## Platform

Solaris, Windows, HP-UX, AIX, Linux

# Integratable Stack

## Service Creation, Assembly, and Deployment UML, BPSS, WSDL, NetBeans

### Service Delivery

WebDAV,  
SyncML, RDF, RSS,  
WML, cHTML,  
J2ME, MIDP,  
JavaCard,  
VoiceXML

### Service Container J2EE

#### Applications/ Core Web Services

ESMTP, IMAP, POP, S/MIME,  
SMS, iCal, SIP, *SIMPLE*

#### Web Services (See right column)

### Service Integration

UDDI, ebXML,  
JMS, Java  
Connectors,  
SQL, JDBC,  
CORBA,  
JavaMail, FTP,  
BPSS, EDI

### Throughout:

HTML, XHTML,  
HTTP(S), SSL/TLS,  
Java, J2SE, J2EE  
(EJB, JSP, Servlets,  
JNDI, JMS, ...), JAX\*  
(JAXM, JAXR, JAX-  
RPC, JAXB, JAXP),  
SOAP, WSDL, XML,  
XSLT, XML Schema,  
SAX, DOM

**Identity and Policy:** *Liberty*, LDAP, *vLIP*, SP-DNA, DSML, UDDI, ebXML, SASL,  
*SAML*, *XACML*, X.509, PKCS, PKIX, OCSP, CIM, CIM-SOAP, WBEM, Kerberos, IKE, JAAS, J2SE  
Policy/Perms, JCA/JCE, P3P, *XKMS*, XML DSIG, XML Encrypt

**Platform:** POSIX, NFS, FTP, Bind, Sendmail, DHCP, TCP, IPv6, Mobile IPv4,  
IPSec, GSS-API, PPP, Fibre Channel, SCSI, *Infiniband*

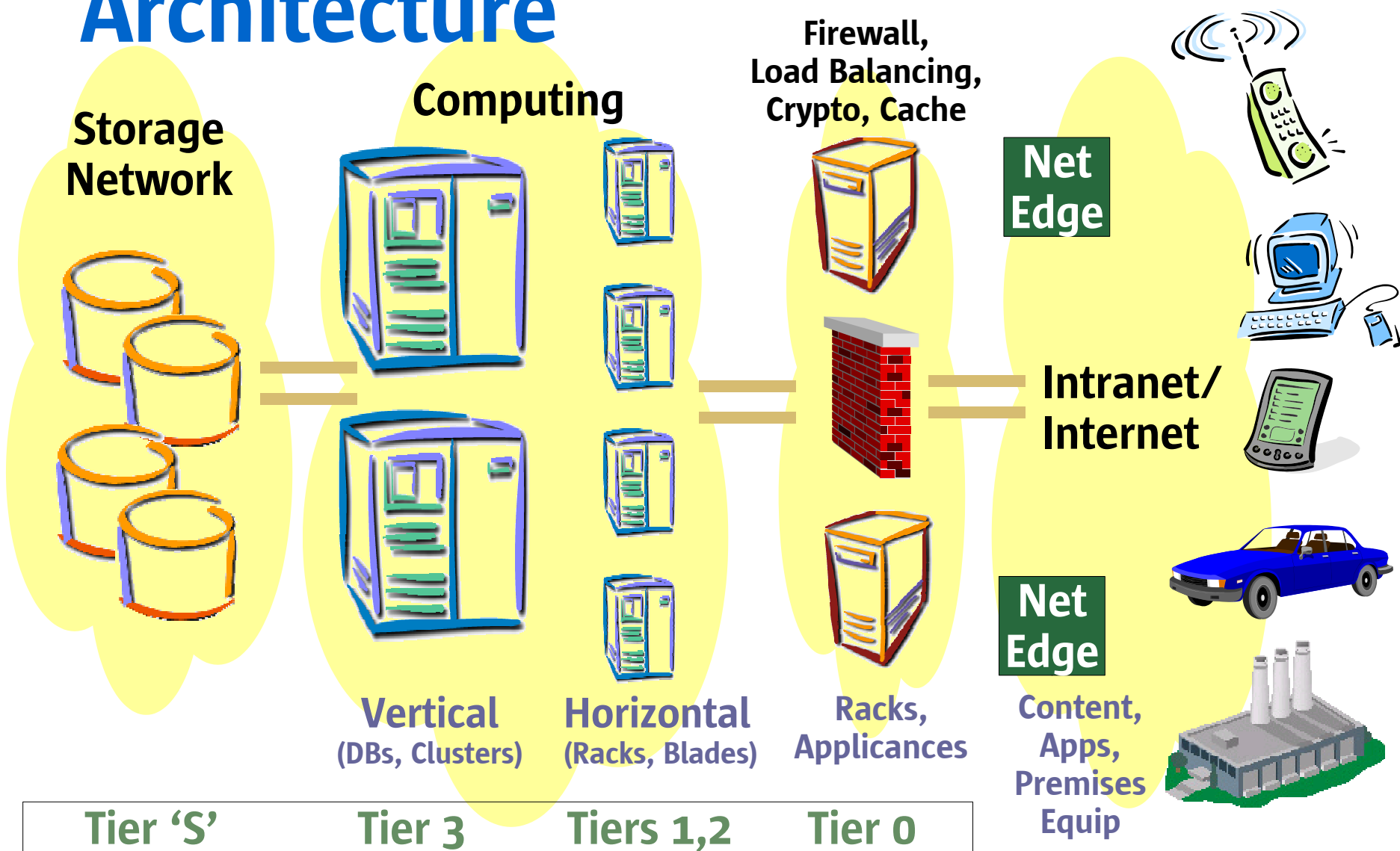
*Italics* == emerging/  
future standard



# Platform: Solaris in DoD

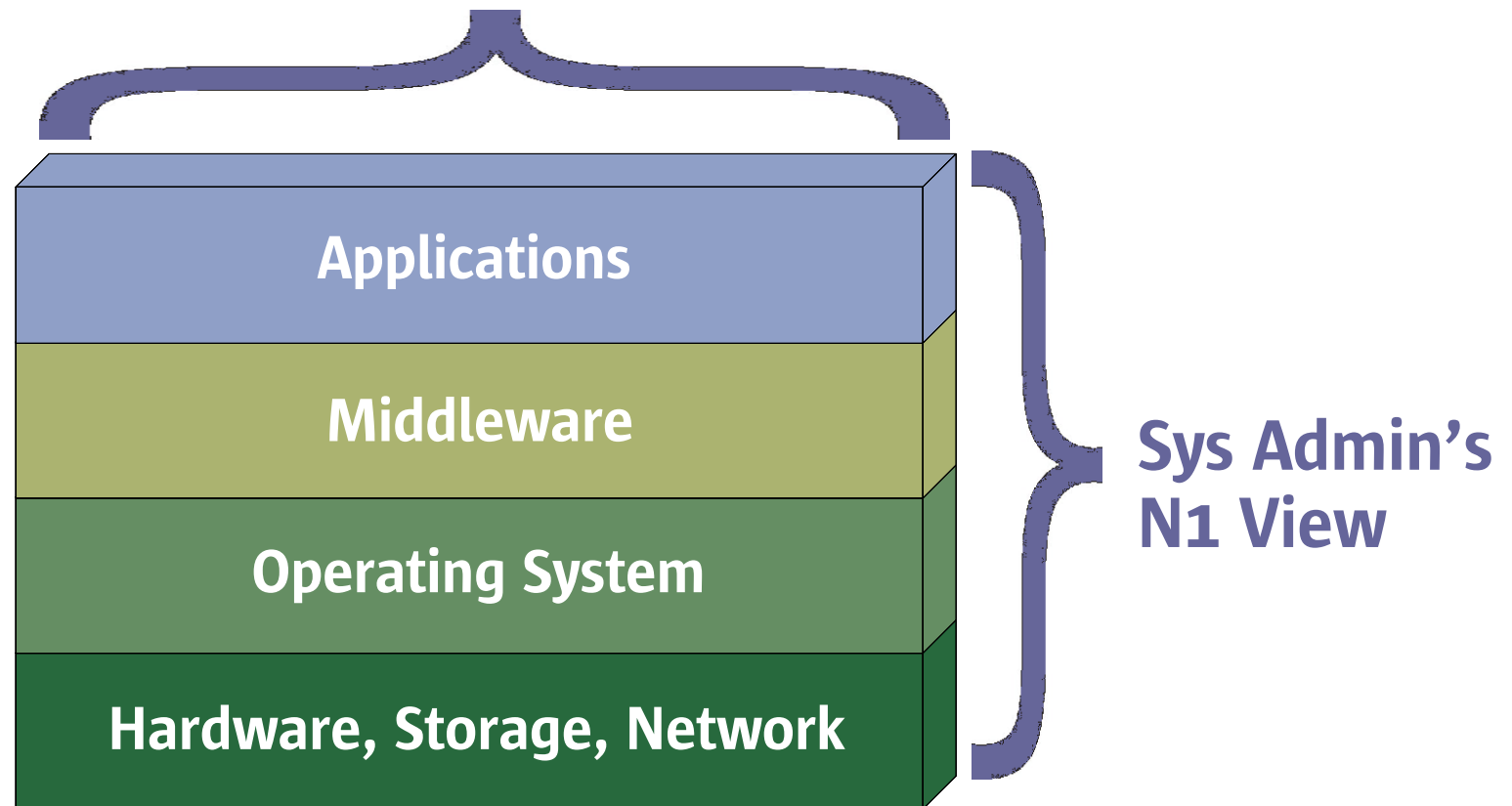
- Trusted Solaris
- Global Command and Control (GCCS)
- Global Combat Support (GCSS)
- Public Key Infrastructure (PKI)
- Global Directory System (GDS)
- Network Intrusion Detection
- Joint Warfare System (JWARS)
- Common Operating Environment (COE)

# N1 Virtual E-to-E Service Architecture



# Complimentary Views

Programmer's Sun ONE View



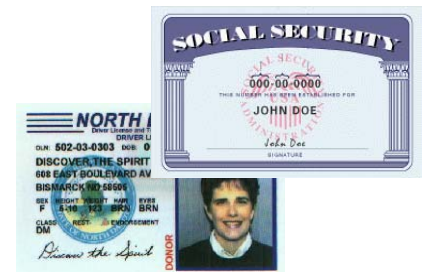
# Network Identity

The set of  
attributes that  
describe profile(s)  
of an individual

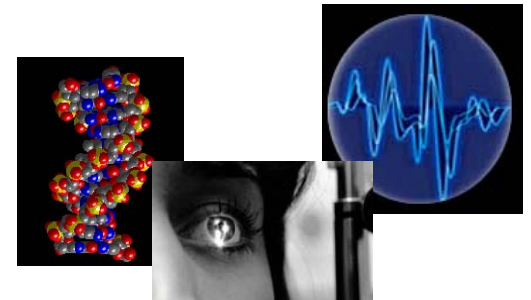
Customer Name  
Email alias  
PIN

John Smith  
jsmith2@freemail.com  
js@eng.sun.com

Credit card number  
Social security number  
Drivers license  
Passport  
Retinal Scan  
DNA

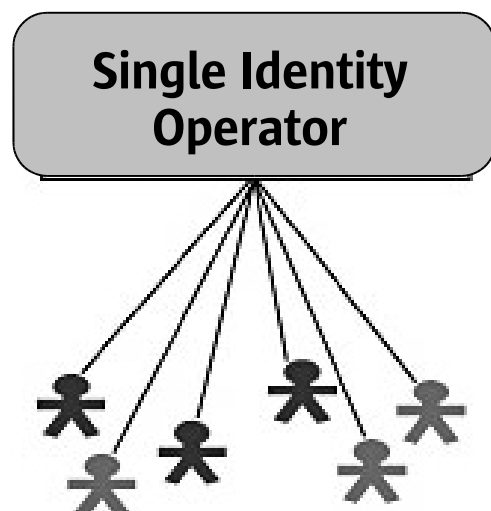


Entertainment preferences  
Notification preferences  
Employee Authorization  
Business Calendar  
Dining preferences  
Affinity program  
Friends and associates  
Education History  
Medical History  
Financial Assets...

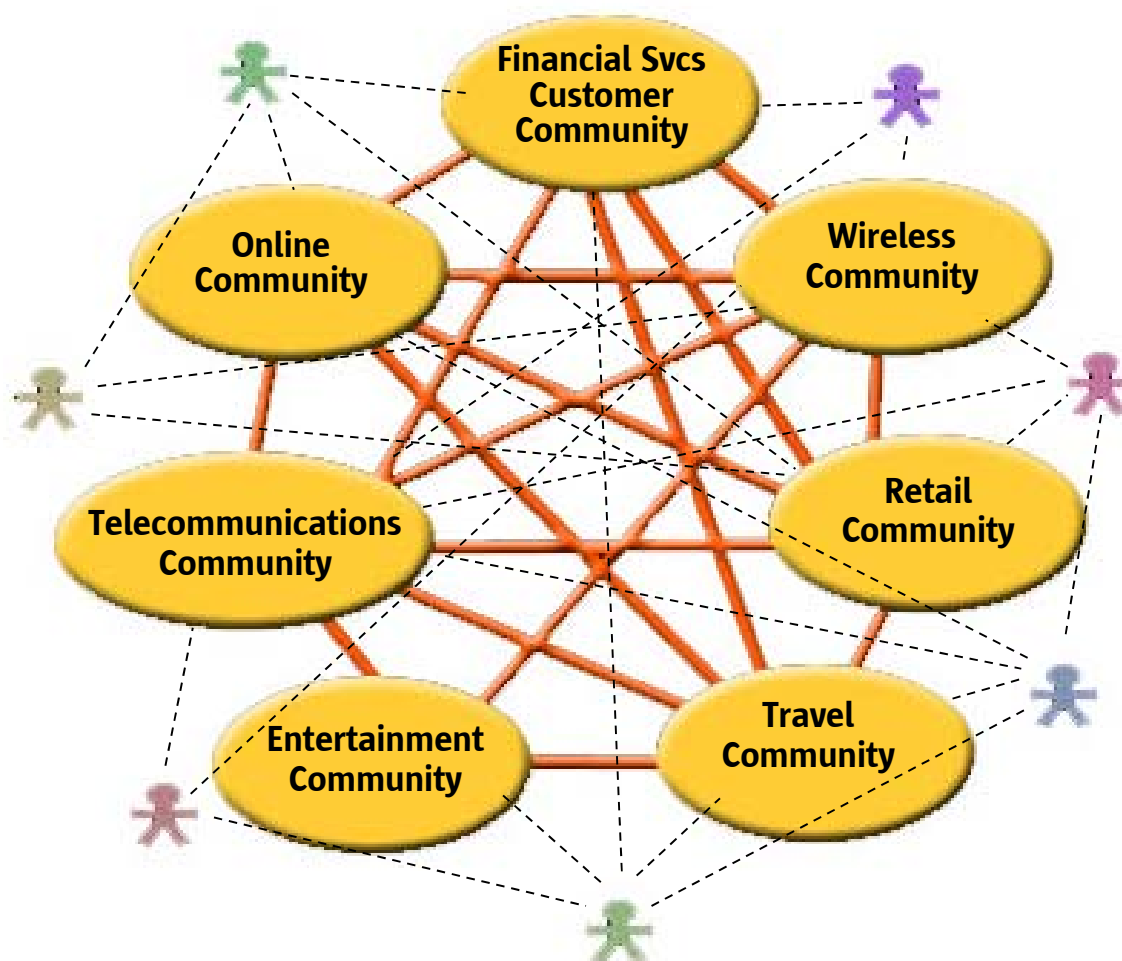


# Possible Identity Solutions

## Centralized Model



## Open Federated Model

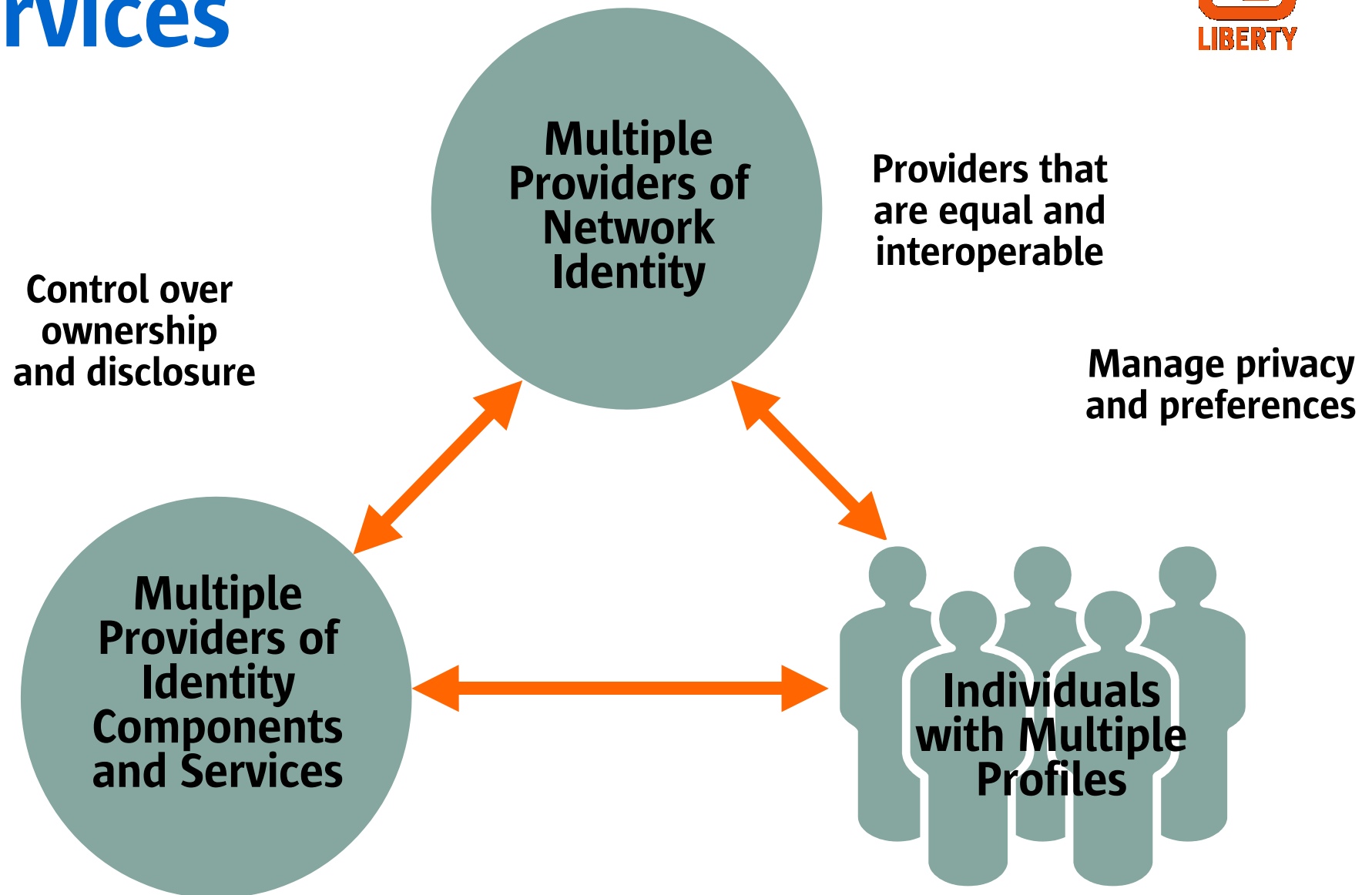


# Liberty Alliance Members > 2,000,000,000 Network Identities



And growing.

# Views of Federated Identity Services





# Defense Manpower Data Center



**November 10, 1999**

**Memo from Dr. John Hamre, Deputy Secretary of Defense**

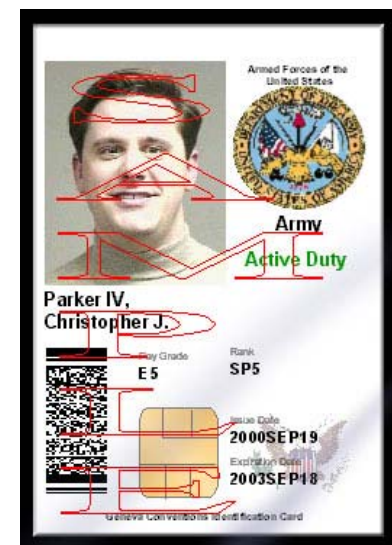
**“ Create a common access card”**

**Challenge:**

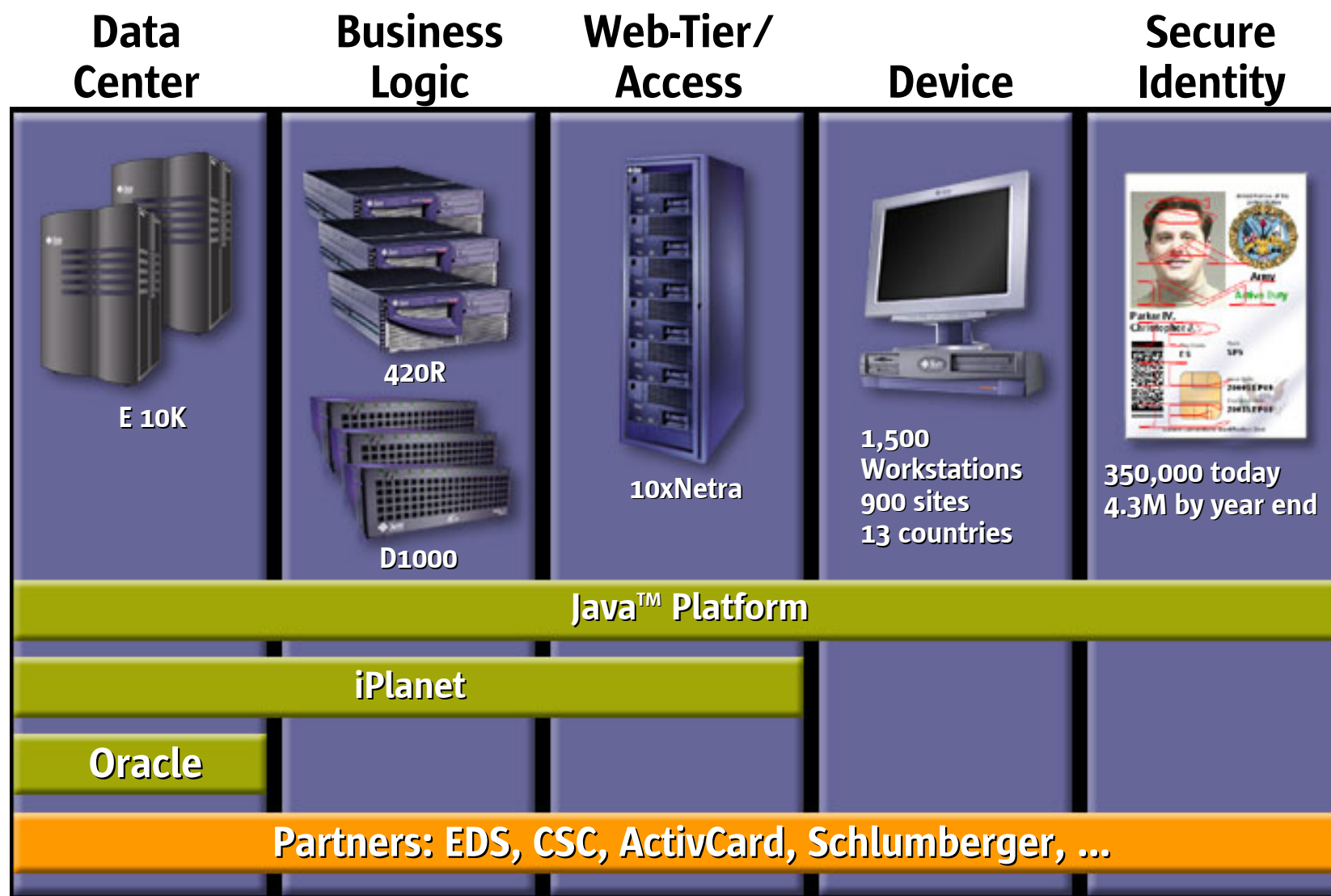
- Reduce redundancy
- Increase security
- Platform for e-business
- Keep it simple

**Result:**

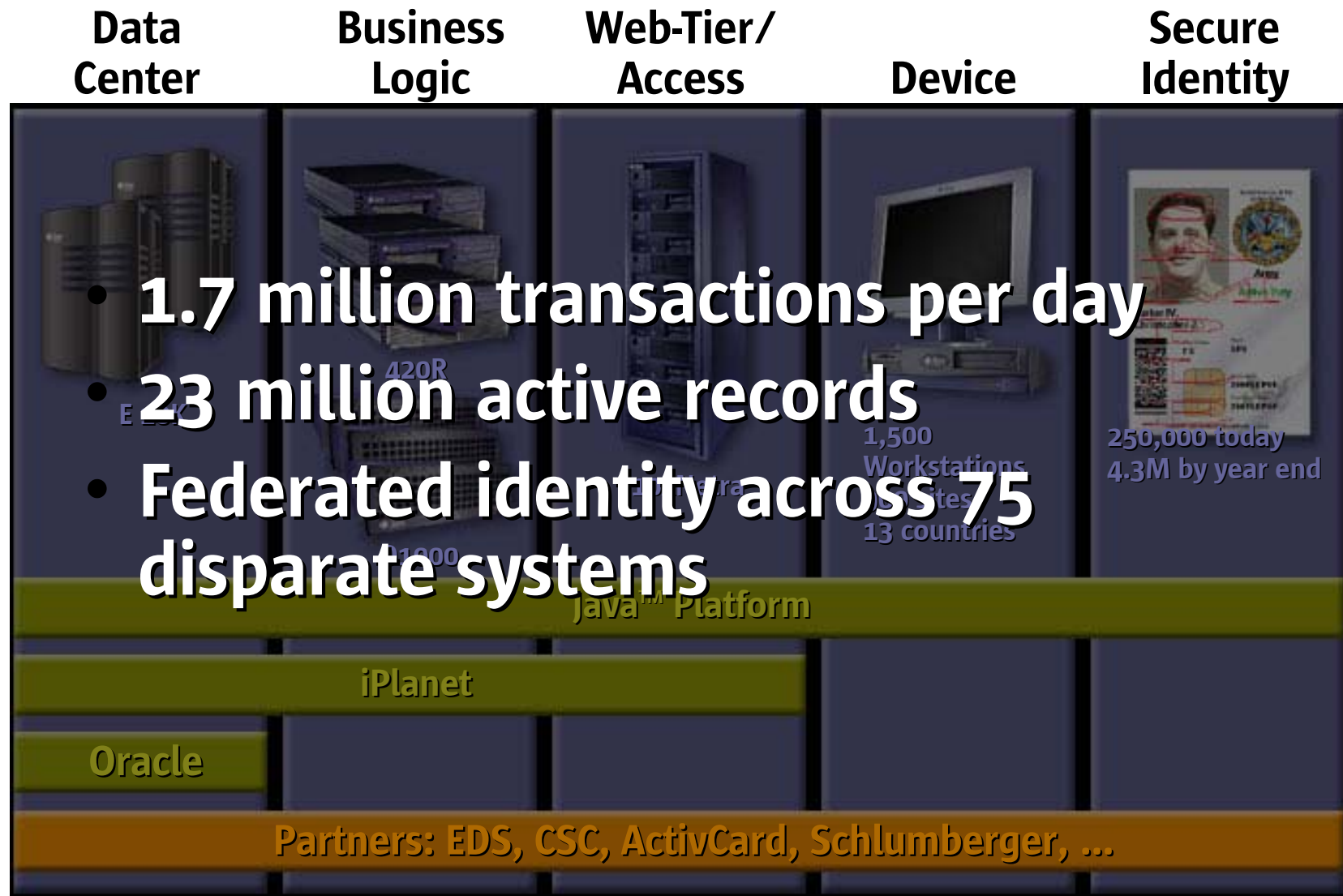
- Production in 12 months
- Single federated identity across 75 systems



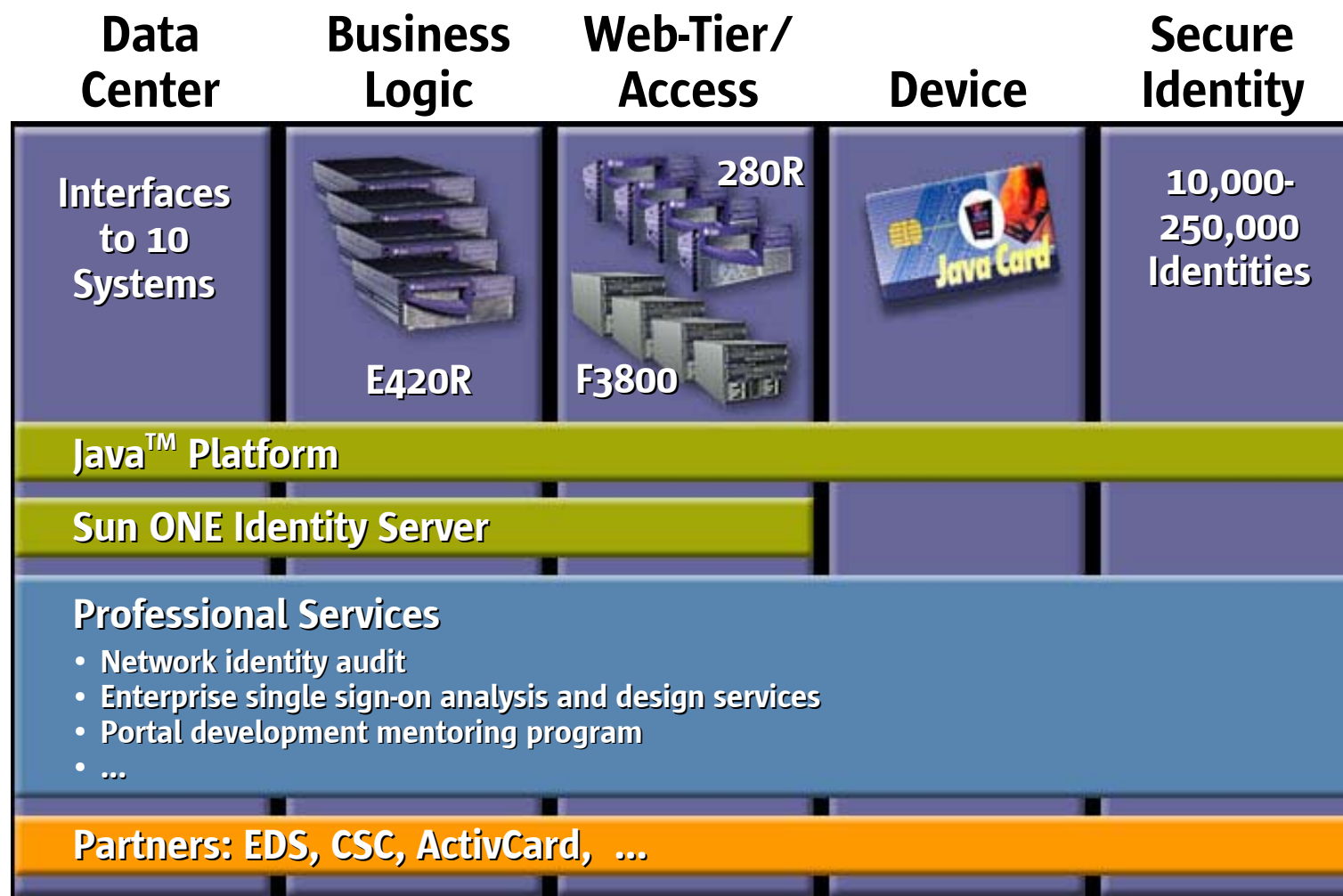
# What DMDC Deployed



# What DMDC Deployed

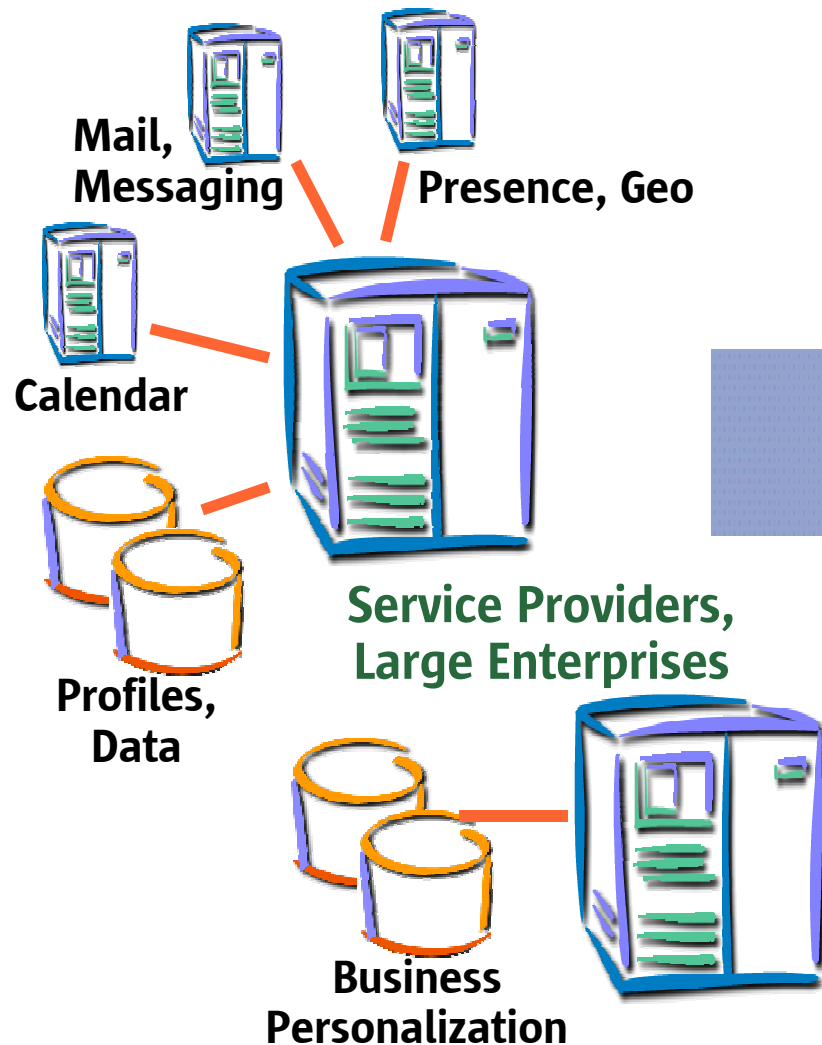


# Sun ONE Platform for Network Identity



First open, secure, scalable Identity Server

# Federated Services



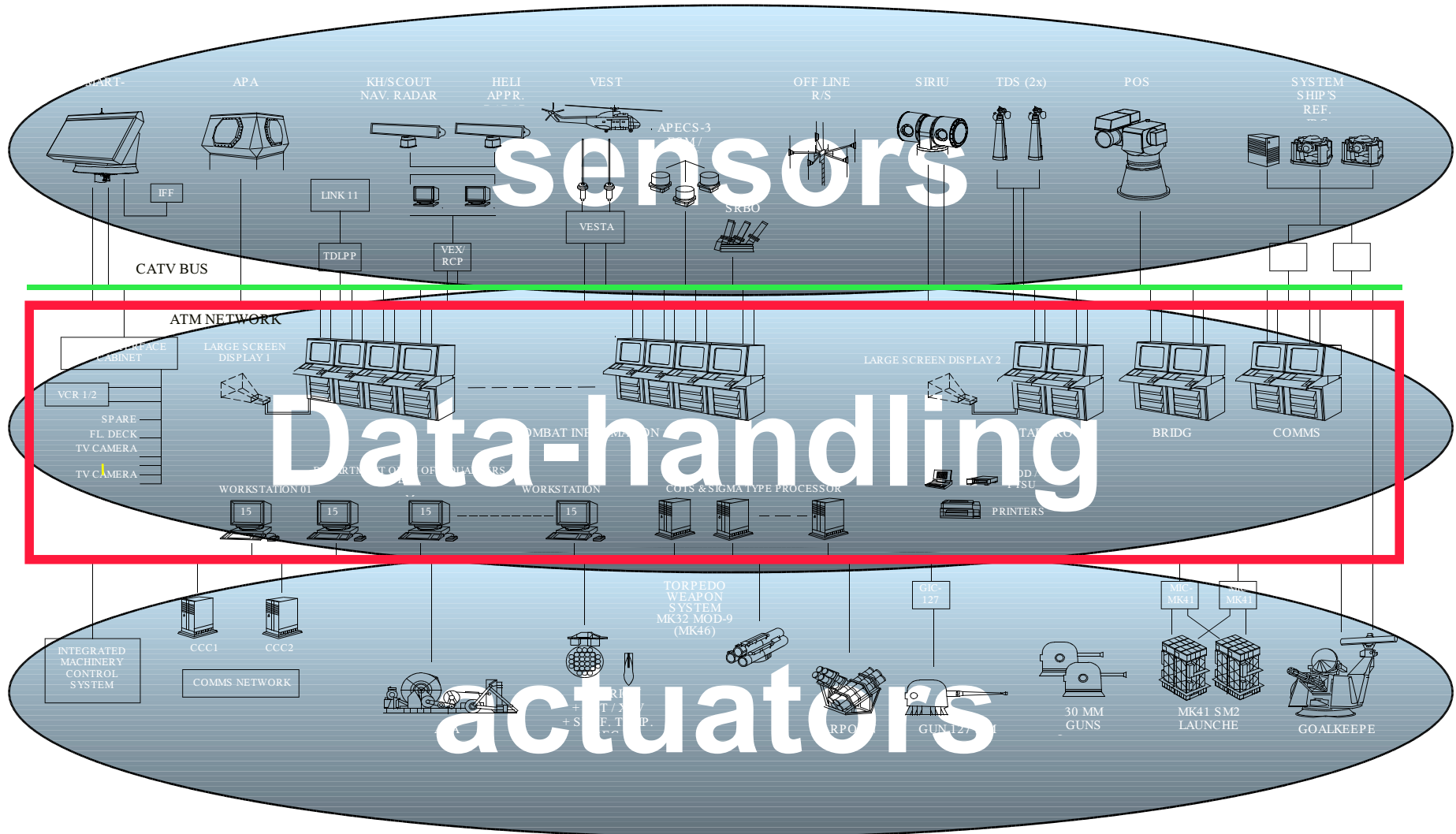
- Ubiquitous context for B2B, B2C, B2E users
- Supports mobility and multi-device access
- Delivered using
  - Open Web Services
  - Federated Identity
  - Standard Schemas
- Built on the SP-grade Sun ONE Comm Backbone
  - Portal, Messaging, Calendar, Collaboration



# Challenges of Dynamic Configurations



# THALES NAVAL NEDERLAND - Surveillance Systems and Weapon Control and Targeting

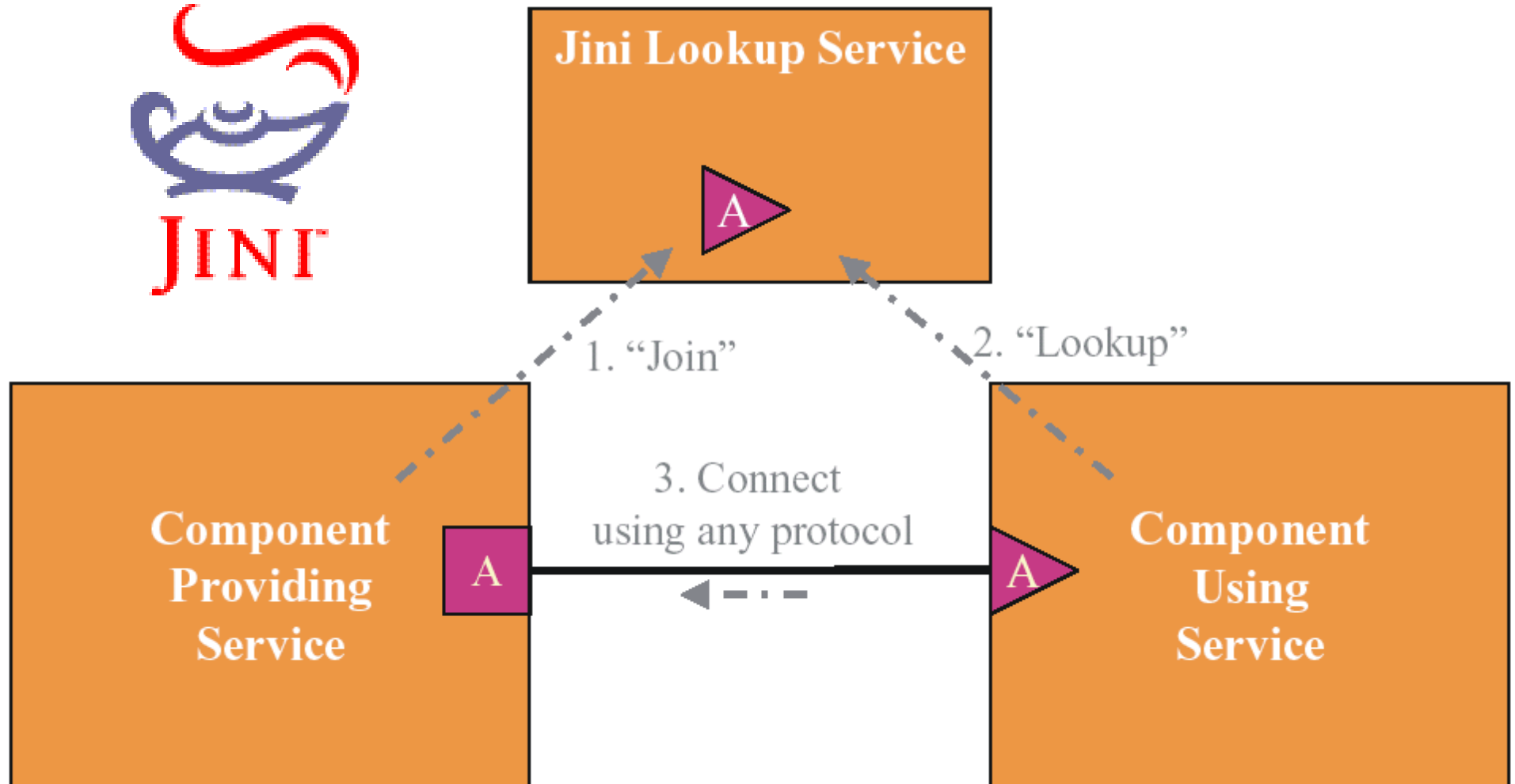




# Challenges of the Battlefield

- Distributed Battlespace with multiple control domains
- Integrate C2 & Weapons systems
- $10^4$ s Decoupled Sensors and Actuators/Shooters
- Reflect State of the World in Real-Time
  - Distribute RT tracks to 'n' nodes; requires performance and scalability
  - Application, Network, Data Transparent
- Rapid Deployment
  - Zero Administration
  - Dynamic Configuration, Self-Healing Networks
- Security: B1 + secure channels

# New Services Architectures: Jini



# New Services Architectures



[www.openwings.org](http://www.openwings.org)

Project  
**RIO**

[rio.jini.org](http://rio.jini.org)

Project  
**JXTA**

[www.jxta.org](http://www.jxta.org)

# Some Tips on Hardening

- Design a Services-Based Architecture
  - Decentralized, resilient, dynamic configurations
- Incorporate Security at Every Point
  - Assume a Byzantine Model
  - Require Federated Identity, Smartcard Strong Authentication
- Build on Open Standards
  - Plan for heterogeneity: platforms and networks
  - Don't put all your eggs in one vendor's basket



**Hal Jespersen**

**hal.jespersen@sun.com**

